World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:1, No:11, 2007



# A New Construction of 16-QAM Codewords with Low Peak Power

Jiaxiang Zhao
Department of Communication Engineering
Nankai University, Weijin Road 94
Tianjin, PRC 300071,
E-mail: zhaojx@nankai.edu.cn

***Abstract*— We present a novel construction of 16-QAM codewords of length $n = 2^k$. The number of constructed codewords is $16^2 \times [4^{k-1} \times k - k + 1]$. When these constructed codewords are utilized as a code in OFDM systems, their peak-to-mean envelope power ratios (PMEPR) are bounded above by $3.6$. The principle of our scheme is illustrated with a four subcarrier example.**

***Index Terms*— Extended Rudin-Shapiro construction, orthogonal frequency division multiplexing (OFDM), peak-to-mean envelope power ratio (PMEPR).**

## I. Introduction

Orthogonal frequency-division multiplexing (OFDM) has increasingly become an attractive technique for the high-bit-rate transmission in a radio environment [6]. A principal impediment to implementing OFDM is the high peak-to-mean envelope power ratios (PMEPR) of the transmitted signals. Given QAM (quadrature amplitude modulation) constellations are widely used in OFDM, it is therefore imperative to study the reduction of PMEPR, especially when symbols are chosen from QAM constellations [3].

A variety of creative ways are proposed to reduce PMEPR of OFDM signals [4], [2], [7], [12], [13]. Of these methods, a promising one introduced in [2] uses block coding, where the desired data codeword is embedded in a larger codeword and only a subset of those larger codewords with low PMEPR bounds is used. This method requires one to perform an exhaustive search for identifying the codewords having low PMEPR bounds in a code, and use a large lookup table for encoding and decoding. For high QAM constellations, these drawbacks could make the implementation of it difficult. One way to overcome these drawbacks is to use the code constructed from Golay complementary codewords [5]. A generalization of Golay complementary codewords with symbols chosen from 16-QAM is reported in [3] where $(16+12k)(k!/2)4^{k+1}$ codewords of length $2^k$ are constructed with their PMEPR bound bounded above by $3.6$. However, for bandwidth-efficient long codes, the code rate of this approach drops dramatically.

In this paper, we present a novel scheme of systematically constructing a set of OFDM signals with their subcarriers modulated by the symbols chosen from a 16-QAM constellation. A total $16^2 \times [4^{k-1} \times k - k + 1]$ distinct codewords of length $n = 2^k$ having their PMEPRs bounded above by $3.6$ are constructed. In contrast with [3], our approach is based on a novel way of extending the Rudin-Shapiro (RS) construction (different from [8], [9]). Utilizing this extended RS construction, we develop a procedure to construct a set of the polynomials. The constructed polynomials are then exploited to produce 16-QAM codewords with desired PMEPR bounds.

This work was supported in part by the National Science Foundation of China under Grant 60474012.

The paper is organized as follows. In Section II, we introduce some notations, review the background materials developed in [10], [11] and then formulate the problem. In Section III, a four-carrier example is utilized to illustrate our construction procedure. In Section IV, the general case is discussed. Proofs of some properties are contained in Appendix I and Appendix II.

## II. Preliminaries

The transmitted OFDM signal is the real part of

$$S_{\boldsymbol{c}}(t) \;=\; \sum_{m=1}^{n} c_m e^{-j2\pi(f_0+m\triangle f)t}, \qquad (1)$$

where $\triangle f$ is an integer multiple of the OFDM symbol rate and $f_0$ is the lowest carrier frequency. $\boldsymbol{c} = (c_1, \ldots, c_n)$ is the complex modulating vector whose entries are taken from a 16-QAM constellation. An admissible modulating vector is called a codeword and the ensemble of all the possible codewords constitutes the code $\mathscr{C}$. The mean power of $S_{\boldsymbol{c}}(t)$ during a symbol period $T$ is

$$\frac{1}{T}\int_0^T |S_{\boldsymbol{c}}(t)|^2 dt \;=\; \|\boldsymbol{c}\|^2 \triangleq \sum_{m=1}^{n} |c_m|^2, \qquad (2)$$

and the mean envelope power $P_{av}(\mathscr{C})$ of a code $\mathscr{C}$ is

$$P_{av}(\mathscr{C}) = \frac{1}{T}\sum_{\boldsymbol{c}\in\mathscr{C}}\int_0^T p(\boldsymbol{c})|S_{\boldsymbol{c}}(t)|^2 dt = \sum_{\boldsymbol{c}\in\mathscr{C}} p(\boldsymbol{c})\|\boldsymbol{c}\|^2, \qquad (3)$$

where $p(\boldsymbol{c})$ is the probability of transmitting codeword $\boldsymbol{c}$. The peak-to-mean envelope power ratio (PMEPR) of a codeword $\boldsymbol{c}$ is defined as

$$\mathrm{PMEPR}(\boldsymbol{c}) \;\triangleq\; \frac{\max_{t\in[0,T]} |S_{\boldsymbol{c}}(t)|^2}{P_{av}(\mathscr{C})}. \qquad (4)$$

Our goal is to systematically construct a set of codewords whose PMEPRs are bounded above by 3.6 where entries of these codewords are modulated by a 16-QAM constellation.

Throughout our discussion, we impose the restriction $n = 2^k$ ($k$ positive integer) and use $\mathbb{C}^* \triangleq \mathbb{C} - \{0\}$ and $S^1 \triangleq \{z \in \mathbb{C} : |z| = 1\}$ where $\mathbb{C}$ denotes the set of complex numbers.

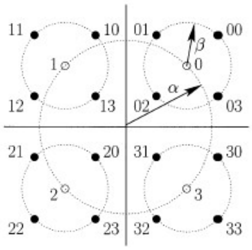


Fig. 1. Construction of 16-QAM symbols from two QPSK symbols

*A. The Extended Rudin-Shapiro Construction*

The extended Rudin-Shapiro map $\Phi^{\alpha\beta\gamma}$ introduced in [10], [11] is defined as follows: Given any polynomial $Q(z)$ ,$\Phi^{\alpha\beta\gamma}$ is

$$\Phi^{\alpha\beta\gamma}(Q(z)) \quad \triangleq \quad \frac{1}{\gamma}\left[\alpha Q(\gamma z^2) + \beta z^{-1} Q(-\gamma z^2)\right] , \quad (5)$$

where we require $\alpha\,,\,\beta \in \mathbb{C}^*$ , and $\gamma \in S^1$ .

In [11], we confine parameters $\alpha\,,\,\beta\,,\,\gamma \in S^1$, develop a procedure to construct $P_k$ of degree $2^k$ and prove

$$|P_k(z\,;\,\alpha_k\,,\,\beta_k\,,\,\gamma_k\,,\,\ldots\,,\,\alpha_1\,,\,\beta_1\,,\,\gamma_1)|^2 + |P_k(-z\,;\,\alpha_k\,,\beta_k\,,\gamma_k\,,\ldots\,,\alpha_1\,,\beta_1\,,\gamma_1)|^2 = 2^{k+1}\ ,\ \forall\, z \in S^1 (6)$$

for any choices of $\alpha_k\,,\beta_k\,,\gamma_k\,,\ldots\,,\alpha_1\,,\beta_1\,,\gamma_1 \in S^1$ .

## III. A Simple Example

A four-carrier OFDM signal of (1) where the entries of $(c_1\,,c_2\,,c_3\,,c_4)$ are chosen from a 16-QAM constellation is used to illustrate our construction procedure. Instead of performing an exhaustive search, as originally described in [2], the procedure we present can efficiently identify a set of codewords whose PMEPR bounds are bounded above by $3.6$ .

*A. A construction procedure*

Based on the procedure developed in [11] or our derivation of Section D, we have a polynomial of degree $4$ represented as:

$$\begin{aligned} &P_2(z\,;\,\alpha_2\,,\,\beta_2\,,\,\gamma_2\,,\,\alpha_1\,,\,\beta_1) \\ &= \gamma_2\alpha_2\alpha_1 z^4 + \gamma_2\beta_2\alpha_1 z^3 - \alpha_2\beta_1 z^2 + \beta_2\beta_1 z\,. \end{aligned} \quad (7)$$

According to [1], any point on the $16$-QAM constellation can be written as

$$q(\mu\,,\,\nu) \quad = \quad a e^{j\pi/4}\xi^{\mu} + b e^{j\pi/4}\xi^{\nu} \quad (8)$$

This representation of a 16-QAM symbol in terms of two QPSK symbols is shown in Fig. $1$ . Assuming all the 16-QAM symbols are equiprobable, we require $a = 2/\sqrt{5}$ and $b = 1/\sqrt{5}$ for the constellation to have unit average energy. Thus, for our example, it can be verified that $P_{\text{av}} = 4$ .

In equation (7), we choose parameters as follows:

$$\begin{aligned} \alpha_1 &= a e^{j\pi/4}\xi^{\mu} + b e^{j\pi/4}\xi^{\nu} \\ \beta_1 &= a e^{j\pi/4}\xi^{\tilde{\mu}} + b e^{j\pi/4}\xi^{\tilde{\nu}} \\ \alpha_2 &= \xi^{\lambda} \\ \beta_2 &= \xi^{\tau} \\ \gamma_2 &= \xi^{\kappa} \end{aligned} \quad (9)$$

where $\mu\,,\,\nu\,,\,\tilde{\mu}\,,\,\tilde{\nu}\,,\,\tau\,,\,\kappa$ and $\lambda$ are chosen from $\mathbb{Z}_4$ .

Thus, equation (7) becomes

$$\begin{aligned} &P_2(z\,;\,\alpha_2\,,\,\beta_2\,,\,\gamma_2\,,\,\alpha_1\,,\,\beta_1) \\ &= \gamma_2\alpha_2\alpha_1 z^4 + \gamma_2\beta_2\alpha_1 z^3 - \alpha_2\beta_1 z^2 + \beta_2\beta_1 z \\ &= \gamma_2\alpha_2(a e^{j\pi/4}\xi^{\mu} + b e^{j\pi/4}\xi^{\nu}) z^4 + \gamma_2\beta_2(a e^{j\pi/4}\xi^{\mu} + b e^{j\pi/4}\xi^{\nu}) z^3 \\ &\quad - \alpha_2(a e^{j\pi/4}\xi^{\tilde{\mu}} + b e^{j\pi/4}\xi^{\tilde{\nu}}) z^2 + \beta_2(a e^{j\pi/4}\xi^{\tilde{\mu}} + b e^{j\pi/4}\xi^{\tilde{\nu}}) z \\ &= \xi^{\kappa}\xi^{\lambda}(a e^{j\pi/4}\xi^{\mu} + b e^{j\pi/4}\xi^{\nu}) z^4 + \xi^{\kappa}\xi^{\tau}(a e^{j\pi/4}\xi^{\mu} + b e^{j\pi/4}\xi^{\nu}) z^3 \\ &\quad + \xi^2\xi^{\lambda}(a e^{j\pi/4}\xi^{\tilde{\mu}} + b e^{j\pi/4}\xi^{\tilde{\nu}}) z^2 + \xi^{\tau}(a e^{j\pi/4}\xi^{\tilde{\mu}} + b e^{j\pi/4}\xi^{\tilde{\nu}}) z \\ &= e^{j\pi/4}\xi^{\mu+\kappa+\lambda}(a + b\xi^{\nu-\mu}) z^4 + e^{j\pi/4}\xi^{\mu+\kappa+\tau}(a + b\xi^{\nu-\mu}) z^3 \\ &\quad + e^{j\pi/4}\xi^{\tilde{\mu}+\lambda+2}(a + b\xi^{\tilde{\nu}-\tilde{\mu}}) z^2 + e^{j\pi/4}\xi^{\tilde{\mu}+\tau}(a + b\xi^{\tilde{\nu}-\tilde{\mu}}) z\,. \end{aligned} \quad (10)$$

We define $\Omega_{2,1}$ as the set of all codewords generated by equation (10) when parameters $\mu\,,\,\nu\,,\,\tilde{\mu}\,,\,\tilde{\nu}\,,\,\tau\,,\,\kappa$ and $\lambda$ run over $\mathbb{Z}_4$ , i.e.,

$$\Omega_{2,1} = \bigcup_{\substack{\mu\,,\,\nu \in \mathbb{Z}_4 \\ \tilde{\nu}\,,\,\tilde{\mu} \in \mathbb{Z}_4 \\ \tau\,,\,\kappa\,,\,\lambda \in \mathbb{Z}_4}} \left\{ \begin{bmatrix} e^{j\pi/4}\xi^{\mu+\kappa+\lambda}(a + b\xi^{\nu-\mu}) \\ e^{j\pi/4}\xi^{\mu+\kappa+\tau}(a + b\xi^{\nu-\mu}) \\ e^{j\pi/4}\xi^{\tilde{\mu}+\lambda+2}(a + b\xi^{\tilde{\nu}-\tilde{\mu}}) \\ e^{j\pi/4}\xi^{\tilde{\mu}+\tau}(a + b\xi^{\tilde{\nu}-\tilde{\mu}}) \end{bmatrix}^{\mathrm{T}} \right\} . \quad (11)$$

We can also choose the parameters of (7) in a way different from (9) to produce more codewords with low PMEPR bounds. Further discussion on this issue, especially, on how to tuning parameter $\gamma$ is presented in another paper.

Here, another choice for the set of parameters in (7) is

$$\begin{aligned} \alpha_1 &= \xi^{\lambda} \\ \beta_1 &= \xi^{\tau} \\ \alpha_2 &= a e^{j\pi/4}\xi^{\mu} + b e^{j\pi/4}\xi^{\nu} \\ \beta_2 &= a e^{j\pi/4}\xi^{\tilde{\mu}} + b e^{j\pi/4}\xi^{\tilde{\nu}} \\ \gamma_2 &= \xi^{\kappa} \end{aligned} \quad (12)$$

where $\mu\,,\,\nu\,,\,\tilde{\mu}\,,\,\tilde{\nu}\,,\,\tau\,,\,\kappa$ and $\lambda$ are chosen from $\mathbb{Z}_4$ . Substituting (12) for parameters in (7), we similarly define $\Omega_{2,2}$ , i.e.,

$$\Omega_2 \quad = \quad \Omega_{2,1} \bigcup \Omega_{2,2}\,. \quad (13)$$

*B. PMEPR bounds*

Now, we compute PMEPR upper bounds for the codewords of (13). For this purpose, we first prove the following lemma.

**Lemma 1:** If $|\alpha_2| = |\beta_2|$ and $\gamma_2 \in S^1$, then the polynomial (7) satisfies

$$\max_{z \in S^1} |P_2(z\,;\,\alpha_2, \beta_2, \gamma_2, \alpha_1, \beta_1)|^2 \le 4(|\alpha_1|^2 + |\beta_1|^2)|\beta_2|^2 . \quad (14)$$

The proof of Lemma 1 is contained in Appendix I.

**Corollary 1:** If $|\alpha_1| = |\beta_1|$ and $\gamma_2 \in S^1$, then the polynomial (7) satisfies

$$\max_{z \in S^1} |P_2(z\,;\,\alpha_2, \beta_2, \gamma_2, \alpha_1, \beta_1)|^2 \le 4(|\alpha_2|^2 + |\beta_2|^2)|\beta_1|^2 . \quad (15)$$

The proof of this corollary is similar to Lemma $1$ .

Because of

$$|a e^{j\pi/4}\xi^{\mu} + b e^{j\pi/4}\xi^{\nu}| = |e^{j\pi/4}\xi^{\mu}(a + b\xi^{\nu-\mu})| = |a + b\xi^{\nu-\mu}| (16)$$

and (recalling $a = 2/\sqrt{5}$ , $b = 1/\sqrt{5}$ and $\xi = e^{j\frac{\pi}{2}}$)

$$|a + b\xi^i|^2 \quad = \quad \begin{cases} |a+b|^2 = 1.8\,, & \text{if } i = 0 \\ |a|^2 + |b|^2 = 1\,, & \text{if } i \in \{1\,,\,3\} \\ |a-b|^2 = 0.2\,, & \text{if } i = 2 \end{cases} \ , \quad (17)$$

in view of (9), it follows

$$|\alpha_1|^2 + |\beta_1|^2 \in \{3.6\,,\,2.8\,,\,2.0\,,\,1.2\,,\,0.4\}\,. \quad (18)$$

Utilizing (18) and (9), we can therefore derive

$$(|\alpha_1|^2+|\beta_1|^2)|\beta_2|^2 \quad = \quad (|\alpha_1|^2+|\beta_1|^2) \leq 3.6 \tag{19}$$

which and Lemma 1 yield

$$\max_{z \in S^1} |P_2(z\,;\,\alpha_2\,,\beta_2\,,\gamma_2\,,\alpha_1\,,\beta_1)|^2 \quad \leq \quad 3.6 \times 4\,. \tag{20}$$

Recalling $P_{\text{av}} = 4$, we prove

$$\text{PMEPR}(\boldsymbol{c}) \quad \leq \quad 3.6 \tag{21}$$

for every codeword $\boldsymbol{c} \in \Omega_{2,1}$.

Utilizing Corollary 1, we can similarly prove (21) for every codeword $\boldsymbol{c} \in \Omega_{2,2}$. In view of (13), we therefore prove (21) for every codeword $\boldsymbol{c} \in \Omega_2$.

### C. The size of $\Omega_2$

To compute the size of $\Omega_2$, we first find the sizes of $\Omega_{2,1}$, $\Omega_{2,2}$ and $\Omega_{2,1} \bigcap \Omega_{2,2}$, and then obtain the size of $\Omega_2$.

**Property 1:** When $\alpha_1$, $\beta_1$, $\alpha_2$, $\beta_2$ and $\gamma_2$ defined by either (9) or (12) are used, the sizes of $\Omega_{2,1}$, $\Omega_{2,2}$ and $\Omega_{2,1} \bigcap \Omega_{2,2}$ are respectively $16^2 \times 4$, $16^2 \times 4$ and $16^2$.

**Proof:** In view of (7), every codeword of $\Omega_2$ can be expressed as

$$\boldsymbol{c} = (\gamma_2\alpha_1\alpha_2 \quad \gamma_2\beta_2\alpha_1 \quad -\alpha_2\beta_1 \quad \beta_2\beta_1) \tag{22}$$

where $\alpha_1$, $\beta_1$, $\alpha_2$, $\beta_2$ and $\gamma_2$ are from either (9) or (12).

**Case 1:** Compute the size of $\Omega_{2,1}$. In this case, the parameters defined in (9) are used, which suggests that both $\alpha_1$ and $\beta_1$ are points on the 16-QAM constellation (Fig. 1) and the rest parameters are selected from a 4-PSK constellation, i.e., $\{1\,,-1\,,j\,,-j\}$. Rewriting (22) as $\alpha_2(\gamma_2\alpha_1 \quad \gamma_2\frac{\beta_2}{\alpha_2}\alpha_1 \quad -\beta_1 \quad \frac{\beta_2}{\alpha_2}\beta_1)$, we observe that the first, third and fourth entry can independently be changed through $\alpha_1$, $\beta_1$ and $\frac{\beta_2}{\alpha_2}$ respectively. Thus, every choice of $\alpha_1$, $\beta_1$ and $\frac{\beta_2}{\alpha_2}$ yields a distinct codeword in $\Omega_{2,1}$. Since there are 16 choices for each of $\alpha_1$ and $\beta_1$ and 4 choices for $\frac{\beta_2}{\alpha_2}$, the size of $\Omega_{2,1}$ is equal to $16^2 \times 4$.

**Case 2:** Compute the size of $\Omega_{2,2}$. In this case, the parameters defined in (12) are used. A similar argument as Case 1 can prove that the size of $\Omega_{2,2}$ is equal to $16^2 \times 4$ too.

**Case 3:** To compute the size of $\Omega_{2,1} \bigcap \Omega_{2,2}$, we assume

$$(\gamma_2\alpha_1\alpha_2 \; \gamma_2\beta_2\alpha_1 \; -\alpha_2\beta_1 \; \beta_2\beta_1) = (\tilde{\gamma}_2\tilde{\alpha}_1\tilde{\alpha}_2 \; \tilde{\gamma}_2\tilde{\beta}_2\tilde{\alpha}_1 \; -\tilde{\alpha}_2\tilde{\beta}_1 \; \tilde{\beta}_2\tilde{\beta}_1) \tag{23}$$

where $\alpha_1$, $\beta_1$, $\alpha_2$, $\beta_2$ and $\gamma_2$ represent the parameters defined by (9) but $\tilde{\alpha}_1$, $\tilde{\beta}_1$, $\tilde{\alpha}_2$, $\tilde{\beta}_2$ and $\tilde{\gamma}_2$ are the parameters defined by (12). The equation (23) suggests

$$\gamma_2\alpha_1\alpha_2 \quad = \quad \tilde{\gamma}_2\tilde{\alpha}_1\tilde{\alpha}_2 \tag{24}$$

$$\gamma_2\beta_2\alpha_1 \quad = \quad \tilde{\gamma}_2\tilde{\beta}_2\tilde{\alpha}_1\,. \tag{25}$$

Dividing (24) by (25), we obtain

$$\frac{\gamma_2\alpha_1\alpha_2}{\gamma_2\beta_2\alpha_1} \quad = \quad \frac{\alpha_2}{\beta_2} = \frac{\tilde{\gamma}_2\tilde{\alpha}_1\tilde{\alpha}_2}{\tilde{\gamma}_2\tilde{\beta}_2\tilde{\alpha}_1} = \frac{\tilde{\alpha}_2}{\tilde{\beta}_2}\,. \tag{26}$$

Since $\alpha_2$ and $\beta_2$ are defined by (9), we have $\frac{\alpha_2}{\beta_2} = \xi^\mu$ for some $\mu \in \mathbb{Z}_4$. Combining this with (26), we obtain

$$\tilde{\alpha}_2 \quad = \quad \xi^\mu \tilde{\beta}_2\,. \tag{27}$$

Now, we are ready to estimate the size of $\Omega_{2,1} \bigcap \Omega_{2,2}$.

- When $|\tilde{\alpha}_2| > 1$, for each fixed $\tilde{\alpha}_2$ there are only 4 choices of $\tilde{\beta}_2$ (Fig. 1) satisfying (27). Since we have 4 choices for each of $\tilde{\alpha}_2$, the total number of choices of these parameters satisfying (27) are $4 \times 4 = 16$.
- When $|\tilde{\alpha}_2| < 1$, a similar argument as $|\tilde{\alpha}_2| > 1$ yields another 16 possible choices of parameters.
- When $|\tilde{\alpha}_2| = 1$, there are 8 distinct choices for each of $\tilde{\alpha}_2$ or $\tilde{\beta}_2$. For each choice of $\tilde{\alpha}_2$, however, there only 4 choices of $\tilde{\beta}_2$ (Fig. 1) satisfying (27). Thus, there are total $8 \times 4 = 32$ choices of these parameters satisfying (27).

Combining Case 1-Case 3, we obtain $16 + 16 + 32 = 64$ codewords satisfying (27). On the other hand, rewriting the codewords in $\Omega_{2,2}$ as $\tilde{\beta}_1(\tilde{\gamma}_2\frac{\tilde{\alpha}_1}{\tilde{\beta}_1}\tilde{\alpha}_2 \quad \tilde{\gamma}_2\tilde{\beta}_2\frac{\tilde{\alpha}_1}{\tilde{\beta}_1} \quad -\tilde{\alpha}_2 \quad \tilde{\beta}_2)$, we observe that for each pair of $\tilde{\alpha}_2$ and $\tilde{\beta}_2$ satisfying (27), there are 4 choices of $\frac{\tilde{\alpha}_1}{\tilde{\beta}_1}$. Therefore, the size of $\Omega_{2,1} \bigcap \Omega_{2,2}$ is $4 \times 64 = 256$. In view of (13) and results from Case 1–Case 3, the number codewords in $\Omega_2$ is at least $16^2 \times 4 + 16^2 \times 4 - 256 = 16^2 \times (4 \times 2 - 1) = 1792$.

### D. Derivation of $P_2(z\,;\,\alpha_2\,,\,\beta_2\,,\,\gamma_2\,,\,\alpha_1\,,\,\beta_1)$

$P_2(z\,;\,\alpha_2\,,\,\beta_2\,,\,\gamma_2\,,\,\alpha_1\,,\,\beta_1)$ can be derived through the following 3 steps.

**Step 1**: For the sake of consistence, we choose $\alpha_0 = \beta_0 = \gamma_0 = 1$. Start with $P_0(z) = z$.

**Step 2**: Substituting $P_0(z) = z$ for $Q(z)$ in (5), we compute

$$\begin{aligned} P_1(z\,;\,\alpha_1\,,\,\beta_1\,,\,\gamma_1) &\triangleq \Phi^{\alpha_1\beta_1\gamma_1}(P_0(z)) \\ &= \frac{1}{\gamma_1}\left[\alpha_1 P_0(\gamma_1 z^2) + \beta_1 z^{-1} P_0(-\gamma_1 z^2)\right] \\ &= \frac{1}{\gamma_1}\left[\alpha_1\gamma_1 z^2 + \beta_1 z^{-1}(-\gamma_1 z^2)\right] \\ &= \alpha_1 z^2 - \beta_1 z\,, \end{aligned} \tag{28}$$

where both $\alpha_1$ and $\beta_1$ belong to $\mathbb{C}^*$. Since $P_1$ is independent of $\gamma_1$, we use $P_1(z;\alpha_1,\beta_1)$ to represent $P_1(z;\alpha_1,\beta_1,\gamma_1)$ from now on. Utilizing (28), for all $z \in S^1$, we compute

$$\begin{aligned} &|P_1(z\,;\,\alpha_1\,,\,\beta_1)|^2 + |P_1(-z\,;\,\alpha_1\,,\,\beta_1)|^2 \\ &= |\alpha_1 z^2 - \beta_1 z|^2 + |\alpha_1(-z)^2 - \beta_1(-z)|^2 \\ &= (\alpha_1 z^2 - \beta_1 z)(\alpha_1 z^2 - \beta_1 z)^* + (\alpha_1 z^2 + \beta_1 z)(\alpha_1 z^2 + \beta_1 z)^* \\ &= |\alpha_1 z^2|^2 - \beta_1 z(\alpha_1 z^2)^* - (\beta_1 z)^*\alpha_1 z^2 + |\beta_1 z|^2 \\ &\quad + |\alpha_1 z^2|^2 + \beta_1 z(\alpha_1 z^2)^* + (\beta_1 z)^*\alpha_1 z^2 + |\beta_1 z|^2 \\ &= 2|\alpha_1|^2|z^2|^2 + 2|\beta_1|^2|z|^2 = 2(|\alpha_1|^2 + |\beta_1|^2) \end{aligned} \tag{29}$$

for all $z \in S^1$. From (29), it follows

$$\begin{aligned} &\max_{z \in S^1}\left\{|P_1(z\,;\,\alpha_1\,,\,\beta_1)|^2 + |P_1(-z\,;\,\alpha_1\,,\,\beta_1)|^2\right\} \\ &= 2(|\alpha_1|^2 + |\beta_1|^2) \end{aligned} \tag{30}$$

for any $z \in S^1$ and for any choice of $\alpha_1$, $\beta_1 \in \mathbb{C}^*$.

**Step 3**: As Step 2, substituting $P_1(z\,;\,\alpha_1\,,\,\beta_1\,,\,\gamma_1) = \alpha_1 z^2 - \beta_1 z$ for $Q(z)$ in (5), we compute

$$\begin{aligned} &P_2(z\,;\,\alpha_2\,,\,\beta_2\,,\,\gamma_2\,,\,\alpha_1\,,\,\beta_1) \\ &\triangleq \Phi^{\alpha_2\beta_2\gamma_2}(P_1(z\,;\,\alpha_1\,,\,\beta_1)) \\ &= \frac{[\alpha_2 P_1(\gamma_2 z^2\,,\,\alpha_1\,,\,\beta_1) + \beta_2 z^{-1} P_1(-\gamma_2 z^2\,,\,\alpha_1\,,\,\beta_1)]}{\gamma_2} \\ &= \frac{[\alpha_2(\alpha_1(\gamma_2 z^2)^2 - \beta_1\gamma_2 z^2) + \beta_2 z^{-1}(\alpha_1(-\gamma_2 z^2)^2 - \beta_1(-\gamma_2 z^2))]}{\gamma_2} \\ &= \frac{1}{\gamma_2}[\alpha_1\alpha_2\gamma_2^2 z^4 - \alpha_2\beta_1\gamma_2 z^2 + \beta_2(\alpha_1\gamma_2^2 z^3 + \beta_1\gamma_2 z)] \\ &= \alpha_1\alpha_2\gamma_2 z^4 + \alpha_1\beta_2\gamma_2 z^3 - \alpha_2\beta_1 z^2 + \beta_1\beta_2 z\,. \end{aligned} \tag{31}$$

for any choices of $\alpha_2$, $\beta_2$, $\alpha_1$ and $\beta_1 \in \mathbb{C}^*$ and $\gamma_2$ in $S^1$.

## IV. 16-QAM Codewords of Length $n = 2^k$ Having Low PMEPR Bounds

In this section, we extend the procedure developed in previous section to construct 16-QAM codewords of length $n = 2^k$ with low PMEPR bounds. Our procedure is proceeded in the following steps:

**Step 1**: For $k = 2$, as shown in previous section, we construct polynomial $P_2$. Then, we define $\Omega_2$ (equation (13)) comprising of all the codewords produced by $P_2(z\,;\alpha_2\,,\beta_2\,,\gamma_2\,,\alpha_1\,,\beta_1)$ when the parameters defined by (9) and (12) are employed. We show that the PMEPR bounds for all the codewords of $\Omega_2$ are bounded above by $3.6$. Furthermore, we prove that the size of $\Omega_2$ is $16^2\times(4\times 2-1)$.

**Step 2**: For $k = l$, assume that we have constructed polynomial $P_l$ of degree $2^l$.

Define the following $l$ sets of the parameters $\alpha_l, \beta_l, \gamma_l, \ldots, \alpha_2, \beta_2, \gamma_2, \alpha_1, \beta_1$ as

$$(1)\begin{cases}\alpha_1 = q(\mu,\nu)\\ \beta_1 = q(\tilde{\mu},\tilde{\nu})\\ \alpha_2 = \xi^{\lambda_1}\\ \beta_2 = \xi^{\tau_1}\\ \gamma_2 = \xi^{\kappa_1}\\ \quad\vdots\\ \alpha_l = \xi^{\lambda_{l-1}}\\ \beta_l = \xi^{\tau_{l-1}}\\ \gamma_l = \xi^{\kappa_{l-1}}\end{cases} \quad\ldots\quad (l)\begin{cases}\alpha_1 = \xi^{\lambda_1}\\ \beta_1 = \xi^{\tau_1}\\ \alpha_2 = \xi^{\lambda_2}\\ \beta_2 = \xi^{\tau_2}\\ \gamma_2 = \xi^{\kappa_1}\\ \quad\vdots\\ \alpha_{l-1} = \xi^{\lambda_{l-1}}\\ \beta_{l-1} = \xi^{\tau_{l-1}}\\ \gamma_{l-1} = \xi^{\kappa_{l-2}}\\ \alpha_l = q(\mu,\nu)\\ \beta_l = q(\tilde{\mu},\tilde{\nu})\\ \gamma_l = \xi^{\kappa_{l-1}}\end{cases} \tag{32}$$

where $\mu, \nu, \tilde{\mu}, \tilde{\nu}, \tau_1, \kappa_1, \lambda_1, \ldots, \tau_{l-1}, \kappa_{l-1}$ and $\lambda_{l-1}$ are chosen from $\mathbb{Z}_4$. As done in (11), we replace the parameters of $P_l(z\,;\alpha_l\,,\beta_l\,,\gamma_l\,,\ldots,\alpha_2\,,\beta_2\,,\gamma_2\,,\alpha_1\,,\beta_1)$ with $(i)$ of (32) $(1 \le i \le l)$ and then define $\Omega_{l,i}$ as the set comprising of all the codewords produced by this polynomial. The set $\Omega_l$ is defined as

$$\Omega_l = \bigcup_{i=1}^{l} \Omega_{l,i}\,. \tag{33}$$

Induction also assumes that the sizes of $\Omega_{l,i}$ $(1 \le i \le l)$ and $\Omega_l$ respectively are $16^2 \times 4^{l-1}$ and $16^2 \times (4^{l-1} \times l - l + 1)$.

**Step 3:** For $k = l+1$, let $P_l$ represent the polynomial of degree $n = 2^l$ constructed in Step 2. Employing (5), we construct the polynomial of degree $n = 2^{l+1}$ as follows:

$$\begin{aligned}&P_{l+1}(z\,;\alpha_{l+1}\,,\beta_{l+1}\,,\gamma_{l+1}\,,\ldots,\alpha_2\,,\beta_2\,,\gamma_2\,,\alpha_1\,,\beta_1)\\ &=\frac{1}{\gamma_{l+1}}\left[\alpha_{l+1}P_l(\gamma_{l+1}z^2)+\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}z^2)\right].\end{aligned} \tag{34}$$

**Lemma 2:** If $\gamma_i \in S^1$ for all $i$ with $2 \le i \le l+1$ and $|\alpha_i| = |\beta_i|$ for all $i$ $(1 \le i \le l+1)$ but some $i_0$ with $1 \le i_0 \le l+1$, then the polynomial (34) satisfies

$$\begin{aligned}&\max_{z\in S^1}|P_{l+1}(z\,;\alpha_{l+1}\,,\beta_{l+1}\,,\gamma_{l+1}\,,\ldots,\alpha_2\,,\beta_2\,,\gamma_2\,,\alpha_1\,,\beta_1)|^2\\ &\le 2^{l+1}(|\alpha_{i_0}|^2+|\beta_{i_0}|^2)\prod_{i=1\,,\,i\neq i_0}^{l+1}|\beta_i|^2\,.\end{aligned} \tag{35}$$

The proof of Lemma 2 is contained in Appendix II.

Define the following $l+1$ sets of the parameters $\alpha_{l+1}, \beta_{l+1}, \gamma_{l+1}, \ldots, \alpha_2, \beta_2, \gamma_2, \alpha_1, \beta_1$ as

$$(1)\begin{cases}\alpha_1 = q(\mu,\nu)\\ \beta_1 = q(\tilde{\mu},\tilde{\nu})\\ \alpha_2 = \xi^{\lambda_1}\\ \beta_2 = \xi^{\tau_1}\\ \gamma_2 = \xi^{\kappa_1}\\ \quad\vdots\\ \alpha_{l+1} = \xi^{\lambda_l}\\ \beta_{l+1} = \xi^{\tau_l}\\ \gamma_{l+1} = \xi^{\kappa_l}\end{cases} \quad\ldots\quad (l+1)\begin{cases}\alpha_1 = \xi^{\lambda_1}\\ \beta_1 = \xi^{\tau_1}\\ \alpha_2 = \xi^{\lambda_2}\\ \beta_2 = \xi^{\tau_2}\\ \gamma_2 = \xi^{\kappa_1}\\ \quad\vdots\\ \alpha_l = \xi^{\lambda_l}\\ \beta_l = \xi^{\tau_l}\\ \gamma_l = \xi^{\kappa_{l-1}}\\ \alpha_{l+1} = q(\tilde{\mu},\tilde{\nu})\\ \beta_{l+1} = q(\tilde{\mu},\tilde{\nu})\\ \gamma_{l+1} = \xi^{\kappa_l}\end{cases} \tag{36}$$

where $\mu$, $\nu$, $\tilde{\mu}$, $\tilde{\nu}$, $\tau_1$, $\kappa_1$, $\lambda_1$, $\ldots$, $\tau_l$, $\kappa_l$ and $\lambda_l$ are chosen from $\mathbb{Z}_4$. As done in (11), we replace the parameters of $P_{l+1}(z\,;\alpha_{l+1}\,,\beta_{l+1}\,,\gamma_{l+1}\,,\ldots,\alpha_2\,,\beta_2\,,\gamma_2\,,\alpha_1\,,\beta_1)$ with $(i)$ of (36) $(1 \le i \le l+1)$ and then define $\Omega_{l+1,i}$ as the set comprising of all the codewords produced by this polynomial. The set $\Omega_{l+1}$ is defined as

$$\Omega_{l+1} = \bigcup_{i=1}^{l+1} \Omega_{l+1,i}\,. \tag{37}$$

### A. PMEPR bounds

We first show that the PMEPR bounds of the codewords in $\Omega_{l+1,1}$ are bounded above by $3.6$. Recalling (17), we have

$$|\alpha_1|^2+|\beta_1|^2 \in \{3.6\,,\,2.8\,,\,2.0\,,\,1.2\,,\,0.4\}\,. \tag{38}$$

Utilizing (35) of Lemma 2 and noticing $\beta_i \in S^1$ for all $i$ $(2 \le i \le l+1)$, we prove

$$\begin{aligned}&\max_{z\in S^1}|P_{l+1}(z\,;\alpha_{l+1}\,,\beta_{l+1}\,,\gamma_{l+1}\,,\ldots,\alpha_2\,,\beta_2\,,\gamma_2\,,\alpha_1\,,\beta_1)|^2\\ &\le 2^{l+1}(|\alpha_1|^2+|\beta_1|^2)\prod_{i=2}^{l+1}|\beta_i|^2 \le 2^{l+1}\times 3.6\,.\end{aligned} \tag{39}$$

Since the codewords of $\Omega_{l+1}$ has length $n = 2^{l+1}$, we have $P_{\rm av} = 2^{l+1}$ which yields

$$\mathrm{PMEPR}(\boldsymbol{c}) \le 3.6 \tag{40}$$

for every codeword $\boldsymbol{c} \in \Omega_{l+1,1}$. Utilizing Lemma 2, we can follow a similar argument to prove (40) for any codeword in $\Omega_{l+1,i}$ $(1 \le i \le l+1)$. Thus, in view of (37), it follows that equation is valid for any codeword in $\Omega_{l+1}$.

### B. The size of $\Omega_{l+1}$

To estimate the size of $\Omega_{l+1}$, we first need to prove the following property.

**Property 2:** The coefficients of the polynomial $P_k(z\,;\alpha_k\,,\beta_k\,,\gamma_k\,,\ldots,\alpha_2\,,\beta_2\,,\gamma_2\,,\alpha_1\,,\beta_1)$ associated with $z^{2^k}$ and $z^{2^k-1}$ are respectively

$$f(\gamma_k\,,\ldots,\gamma_2)\prod_{i=1}^{k}\alpha_i \qquad h(\gamma_k\,,\ldots,\gamma_2)\beta_k\prod_{i=1}^{k-1}\alpha_i \tag{41}$$

where $f$ and $h$ both represent products of the powers of $\gamma_i$ $(2 \le i \le k)$.

**Proof:** We proceed our proof through induction.

- For $k = 2$, in view of (7), Property 2 is valid for the coefficients of $P_2$ associated with $z^4$ and $z^3$.

• For $k = l$, assume that the coefficients of $P_l(z\,;\alpha_l\,,\beta_l\,,\gamma_l\,,\ldots,\alpha_2\,,\beta_2\,,\gamma_2\,,\alpha_1\,,\beta_1)$ associated with $z^{2^k}$ and $z^{2^k-1}$ are respectively

$$f(\gamma_l\,,\ldots,\gamma_2)\prod_{i=1}^{l}\alpha_i \quad h(\gamma_l\,,\ldots,\gamma_2)\beta_l\prod_{i=1}^{l-1}\alpha_i \tag{42}$$

where $f$ and $h$ are defined as stated in Property 2.

• For $k = l+1$, from equation (34), we see that the coefficients of $P_{l+1}$ associated with $z^{2^k}$ and $z^{2^k-1}$ are respectively equal to the leading coefficients of $\frac{\alpha_{l+1}}{\gamma_{l+1}}P_l(\gamma_{l+1}z^2)$ and $\frac{\beta_{l+1}}{\gamma_{l+1}}P_l(-\gamma_{l+1}z^2)$. Thus, utilizing the induction assumption (42), we compute the coefficients of $P_{l+1}$ associated with $z^{2^{l+1}}$ and $z^{2^{l+1}-1}$ respectively as follows:

$$\begin{aligned}\frac{\alpha_{l+1}}{\gamma_{l+1}}\gamma_{l+1}^{2^l}f(\gamma_l,\ldots,\gamma_2)\prod_{i=1}^{l}\alpha_i&=\hat{f}(\gamma_{l+1},\ldots,\gamma_2)\prod_{i=1}^{l+1}\alpha_i\\ \frac{\beta_{l+1}}{\gamma_{l+1}}(-\gamma_{l+1})^{2^l}f(\gamma_l,\ldots,\gamma_2)\prod_{i=1}^{l}\alpha_i&=\hat{h}(\gamma_{l+1},\ldots,\gamma_2)\beta_{l+1}\prod_{i=1}^{l}\alpha_i\end{aligned} \tag{43}$$

This completes our proof.

Now, we are ready to estimate the size of $\Omega_{l+1}$. To do that, we first prove the following property.

**Property 3:** When the parameters of $P_{l+1}(z\,;\alpha_{l+1}\,,\beta_{l+1}\,,\gamma_{l+1}\,,\ldots,\alpha_2\,,\beta_2\,,\gamma_2\,,\alpha_1\,,\beta_1)$ are replaced with the numbers from $(i)$ of (36) $(1\le i\le l+1)$, the sizes of $\Omega_{l+1,i}$ and $(\bigcup_{i=1}^{l}\Omega_{l+1,i})\bigcap\Omega_{l+1,l+1}$ respectively are $16^2\times 4^l$ and $16^2$.

**Proof:** We proceed with our proof through the following cases.

**Case 1:** Compute the size of $\Omega_{l+1,i}$ $(1\le i\le l)$. In this case, the set $(i)$ of (36) is selected, which suggests that $\frac{\beta_{l+1}}{\alpha_{l+1}}$ belongs to $\{1\,,-1\,,j\,,-j\}$. In (34), we see that a choice of $\{P_l\,,\frac{\beta_{l+1}}{\alpha_{l+1}}\}$ yields a distinct $P_{l+1}$ (A similar proof for the parameters chosen from a BPSK constellation can be found in [10]). From the induction assumption of Step 2, there are $16^2\times 4^{l-1}$ distinct $P_l$ (the size of $\Omega_{l,i}$) which suggests that the number of codewords in $\Omega_{l+1,i}$ is $16^2\times 4^{l-1}\times 4=16^2\times 4^l$.

**Case 2:** Compute the size of $\Omega_{l+1,l+1}$. In this case, the set $(l+1)$ of (36) is selected, which implies that all the parameters but $\alpha_{l+1}$ and $\beta_{l+1}$ are selected from a 4-PSK constellation. When all the parameters chosen from a 4-PSK constellation, following the same induction argument of Step 1–Step 3 or utilizing a similar argument in [10], we can prove that there are $4^{l+1}$ distinct $P_l$ of degree $2^l$. In addition, a straightforward argument can show that when the argument of $\frac{\beta_{l+1}}{\alpha_{l+1}}$ is not $\frac{\pi}{2}$, a choice of $\{P_l\,,\beta_{l+1}\,,\alpha_{l+1}\}$ yields a distinct $P_{l+1}$. From Fig. 1, for each choice of $\alpha_{l+1}$, there are 4 choices of $\beta_{l+1}$ that meet this requirement. Thus, there are $4^{l+1}\times 16\times 4=16^2\times 4^l$ choices of $\{P_l\,,\beta_{l+1}\,,\alpha_{l+1}\}$ which yield distinct $P_{l+1}$. The size of $\Omega_{l+1,l+1}$ is $16^2\times 4^l$.

**Case 3:** Compute the size of $(\bigcup_{i=1}^{l}\Omega_{l+1,i})\bigcap\Omega_{l+1,l+1}$. For any codeword of $(\bigcup_{i=1}^{l}\Omega_{l+1,i})\bigcap\Omega_{l+1,l+1}$, we have

$$\begin{aligned}&P_{l+1}(z;\alpha_{l+1},\beta_{l+1},\gamma_{l+1},\ldots,\alpha_2,\beta_2,\gamma_2,\alpha_1\,,\beta_1)\\ &=P_{l+1}(z\,;\tilde{\alpha}_{l+1},\tilde{\beta}_{l+1},\tilde{\gamma}_{l+1},\ldots,\tilde{\alpha}_2\,,\tilde{\beta}_2\,,\tilde{\gamma}_2\,,\tilde{\alpha}_1\,,\tilde{\beta}_1)\end{aligned} \tag{44}$$

where $\alpha_i\,,\beta_i\,,\gamma_i$ $(1\le i\le l+1)$ are from $(t)$ of (36) $(1\le t\le l)$ and $\tilde{\alpha}_i\,,\tilde{\beta}_i\,,\tilde{\gamma}_i$ $(1\le i\le l+1)$ are from $(l+1)$ of (36). Equation (44) suggests that the individual summands of these two polynomials must be equal. In particular, the coefficients associated with $z^{2^l}$ and $z^{2^{l-1}}$ must be equal, which, in view of (41) of Property 2, yields

$$f(\gamma_{l+1}\,,\ldots,\gamma_2)\prod_{i=1}^{l+1}\alpha_i=f(\tilde{\gamma}_{l+1}\,,\ldots,\tilde{\gamma}_2)\prod_{i=1}^{l+1}\tilde{\alpha}_i \tag{45}$$

$$h(\gamma_{l+1},\ldots,\gamma_2)\beta_{l+1}\prod_{i=1}^{l}\alpha_i=h(\tilde{\gamma}_{l+1},\ldots,\tilde{\gamma}_2)\tilde{\beta}_{l+1}\prod_{i=1}^{l}\tilde{\alpha}_i \tag{46}$$

For these parameters are nonzero, dividing (45) by (46) renders

$$\frac{f(\gamma_{l+1},\ldots,\gamma_2)\prod_{i=1}^{l+1}\alpha_i}{h(\gamma_{l+1},\ldots,\gamma_2)\beta_{l+1}\prod_{i=1}^{l}\alpha_i}=\frac{f(\tilde{\gamma}_{l+1},\ldots,\tilde{\gamma}_2)\prod_{i=1}^{l+1}\tilde{\alpha}_i}{h(\tilde{\gamma}_{l+1},\ldots,\tilde{\gamma}_2)\tilde{\beta}_{l+1}\prod_{i=1}^{l}\tilde{\alpha}_i} \tag{47}$$

Simplifying this equation, we obtain

$$\frac{f(\gamma_{l+1}\,,\ldots,\gamma_2)}{h(\gamma_{l+1}\,,\ldots,\gamma_2)}\frac{\alpha_{l+1}}{\beta_{l+1}} = \frac{f(\tilde{\gamma}_{l+1}\,,\ldots,\tilde{\gamma}_2)}{h(\tilde{\gamma}_{l+1}\,,\ldots,\tilde{\gamma}_2)}\frac{\tilde{\alpha}_{l+1}}{\tilde{\beta}_{l+1}} \tag{48}$$

Since parameters $\gamma_i\,,\tilde{\gamma}_i\,,\alpha_{l+1}$ and $\beta_{l+1}$ are all chosen from a 4 constellation (not from $(l+1)$ of (36)), and functions $f$ and $g$ are products of powers of $\gamma_i$ $(2\le i\le l+1)$, we have

$$\{\frac{f(\gamma_{l+1},\ldots,\gamma_2)}{h(\gamma_{l+1},\ldots,\gamma_2)}\frac{\alpha_{l+1}}{\beta_{l+1}},\frac{f(\tilde{\gamma}_{l+1},\ldots,\tilde{\gamma}_2)}{h(\tilde{\gamma}_{l+1},\ldots,\tilde{\gamma}_2)}\}\subseteq\{1,-1,-j,j\} \tag{49}$$

Combining (48)–(49), it follows that

$$\tilde{\alpha}_{l+1} = \xi^{\mu}\tilde{\beta}_{l+1}\,,\quad \mu\in\mathbb{Z}_4\,. \tag{50}$$

Clearly, equation (50) is similar to (27). Therefore, an argument similar to the one for computing the size of $\Omega_{2,1}\bigcap\Omega_{2,2}$ proves that the size of $(\bigcup_{i=1}^{l}\Omega_{l+1,i})\bigcap\Omega_{l+1,l+1}$ is $16^2$. Thus, the number of distinct codewords contained in $\Omega_l$ is at least $16^2\times 4^l\times(l+1)-16^2 l=16^2\times[4^l\times(l+1)-l]$.

## V. Conclusion

We present a novel construction of 16-QAM codewords of length $n=2^k$. The number of constructed codewords is $16^2\times[4^{k-1}\times k-k+1]$. When these constructed codewords are utilized as a code in OFDM systems, their peak-to-mean envelope power ratios (PMEPR) are bounded above by 3.6. The principle of our scheme is illustrated with a four subcarrier example.

## Appendix I
## Proof of Lemma 1

**The proof of Lemma 1:** From (5) and $\gamma_2\in S^1$, it follows

$$\begin{aligned}&|P_2(z\,;\alpha_2,\beta_2,\gamma_2,\alpha_1,\beta_1)|^2+|P_2(-z\,;\alpha_2,\beta_2,\gamma_2,\alpha_1,\beta_1)|^2\\
&=\frac{|\alpha_2P_1(\gamma_2z^2\,;\alpha_1,\beta_1)+\beta_2z^{-1}P_1(-\gamma_2z^2\,;\alpha_1,\beta_1)|^2}{|\gamma_2|}\\
&+\frac{|\alpha_2P_1(\gamma_2(-z)^2;\alpha_1,\beta_1)-\beta_2z^{-1}P_1(-\gamma_2(-z)^2;\alpha_1,\beta_1)|^2}{|\gamma_2|}\\
&=|\alpha_2|^2|P_1(\gamma_2z^2\,;\alpha_1\,,\beta_1)|^2\\
&\quad+\alpha_2P_1(\gamma_2z^2\,;\alpha_1\,,\beta_1)[\beta_2z^{-1}P_1(-\gamma_2z^2\,;\alpha_1\,,\beta_1)]^*\\
&\quad+[\alpha_2P_1(\gamma_2z^2\,;\alpha_1\,,\beta_1)]^*\beta_2z^{-1}P_1(-\gamma_2z^2\,;\alpha_1\,,\beta_1)\\
&\quad+|\beta_2|^2|z^{-1}P_1(-\gamma_2z^2;\alpha_1,\beta_1)|^2+|\alpha_2|^2|P_1(\gamma_2z^2;\alpha_1,\beta_1)|^2\\
&\quad-\alpha_2P_1(\gamma_2z^2\,;\alpha_1\,,\beta_1)[\beta_2z^{-1}P_1(-\gamma_2z^2\,;\alpha_1\,,\beta_1)]^*\\
&\quad-[\alpha_2P_1(\gamma_2z^2\,;\alpha_1\,,\beta_1)]^*\beta_2z^{-1}P_1(-\gamma_2z^2\,;\alpha_1\,,\beta_1)\\
&\quad+|\beta_2|^2|z^{-1}P_1(-\gamma_2z^2\,;\alpha_1\,,\beta_1)|^2\\
&=2|\alpha_2|^2|P_1(\gamma_2z^2;\alpha_1,\beta_1)|^2+2|\beta_2|^2|z^{-1}||P_1(-\gamma_2z^2;\alpha_1,\beta_1)|^2\end{aligned} \tag{51}$$

By requiring $|\alpha_2|=|\beta_2|$, equation (51) becomes

$$2|\beta_2|^2(|P_1(\gamma_2z^2;\,\alpha_1,\beta_1)|^2+|P_1(-\gamma_2z^2;\,\alpha_1,\beta_1)|^2)\,. \tag{52}$$

On the other hand, since $z \in S^1$ and $\gamma_2 \in S^1$ suggest $\gamma_2 z^2 \in S^1$, from (29) it follows

$$|P_1(\gamma_2 z^2;\alpha_1,\beta_1)|^2+|P_1(-\gamma_2 z^2;\alpha_1,\beta_1)|^2=2(|\alpha_1|^2+|\beta_1|^2)\,, \quad (53)$$

$\forall\, z \in S^1$. Combining (52) and (53), we prove

$$\begin{aligned}&|P_2(z\,;\,\alpha_2,\beta_2,\gamma_2,\alpha_1,\beta_1)|^2+|P_2(-z\,;\,\alpha_2,\beta_2,\gamma_2,\alpha_1,\beta_1)|^2\\&= 4(|\alpha_1|^2+|\beta_1|^2)|\beta_2|^2 \qquad (54)\end{aligned}$$

which suggests

$$\begin{aligned}&\max_{z\in S^1}|P_2(z\,;\,\alpha_2\,,\,\beta_2\,,\,\gamma_2\,,\,\alpha_1\,,\,\beta_1)|^2\\&\le \max_{z\in S^1}\big\{|P_2(z\,;\,\alpha_2\,,\,\beta_2\,,\,\gamma_2\,,\,\alpha_1\,,\,\beta_1)|^2\\&\qquad +|P_2(-z\,;\,\alpha_2\,,\,\beta_2\,,\,\gamma_2\,,\,\alpha_1\,,\,\beta_1)|^2\big\}\\&=\ 4(|\alpha_1|^2+|\beta_1|^2)|\beta_2|^2 \qquad (55)\end{aligned}$$

## APPENDIX II
## PROOF OF LEMMA 2

Without loss of generality, we use induction to prove the case where the parameters are chosen from $(1)$ of (36).

**Step 1:** For $k=2$, we have proved that when $|\alpha_2|=|\beta_2|$ and $\gamma_2 \in S^1$, equation (54) is valid in Appendix I, i.e.

$$\begin{aligned}&|P_2(z\,;\,\alpha_2,\beta_2,\gamma_2,\alpha_1,\beta_1)|^2+|P_2(-z\,;\,\alpha_2,\beta_2,\gamma_2,\alpha_1,\beta_1)|^2\\&= 4(|\alpha_1|^2+|\beta_1|^2)|\beta_2|^2\,. \qquad (56)\end{aligned}$$

**Step 2:** For $k \le l$, assume that when $|\alpha_i|=|\beta_i|$ and $\gamma_i \in S^1$ with $i \in \{2\,,\,\dots\,,\,l\}$, we have

$$\begin{aligned}&|P_l(z;\,\alpha_l,\beta_l,\gamma_l,\dots,\alpha_2,\beta_2,\gamma_2,\alpha_1,\beta_1)|^2\\&\quad+|P_l(-z;\alpha_l,\beta_l,\gamma_l,\dots,\alpha_2,\beta_2,\gamma_2,\alpha_1,\beta_1)|^2\\&= 2^l(|\alpha_1|^2+|\beta_1|^2)\prod_{i=2}^{l}|\beta_i|^2 \qquad (57)\end{aligned}$$

for $z \in S^1$.

**Step 3:** For $k=l+1$, we compute

$$\begin{aligned}&|P_{l+1}(z\,;\,\alpha_{l+1},\beta_{l+1},\gamma_{l+1},...,\alpha_1,\beta_1)|^2\\&+|P_{l+1}(-z\,;\,\alpha_{l+1},\beta_{l+1},\gamma_{l+1},...,\alpha_1,\beta_1)|^2\\&=\frac{|\alpha_{l+1}P_l(\gamma_{l+1}z^2)+\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}z^2)|^2}{|\gamma_{l+1}|}\\&+\frac{|\alpha_{l+1}P_l(\gamma_{l+1}(-z)^2)-\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}(-z)^2)|^2}{|\gamma_{l+1}|}\\&=\big[\alpha_{l+1}P_l(\gamma_{l+1}z^2)+\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}z^2)\big]\\&\quad\times\big[\alpha_{l+1}P_l(\gamma_{l+1}z^2)+\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}z^2)\big]^*\\&\quad+\big[\alpha_{l+1}P_l(\gamma_{l+1}z^2)-\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}z^2)\big]\\&\quad\times\big[\alpha_{l+1}P_l(\gamma_{l+1}z^2)-\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}z^2)\big]^*\\&=|\alpha_{l+1}|^2|P_l(\gamma_{l+1}z^2)|^2\\&\quad+\alpha_{l+1}P_l(\gamma_{l+1}z^2)[\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}z^2)]^*\\&\quad+\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}z^2)[\alpha_{l+1}P_l(\gamma_{l+1}z^2)]^*\\&\quad+|\beta_{l+1}z^{-1}|^2|P_l(-\gamma_{l+1}z^2)|^2+|\alpha_{l+1}|^2|P_l(\gamma_{l+1}z^2)|^2\\&\quad-\alpha_{l+1}P_l(\gamma_{l+1}z^2)[\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}z^2)]^*\\&\quad-\beta_{l+1}z^{-1}P_l(-\gamma_{l+1}z^2)[\alpha_{l+1}P_l(\gamma_{l+1}z^2)]^*\\&\quad+|\beta_{l+1}z^{-1}|^2|P_l(-\gamma_{l+1}z^2)|^2\\&=2|\alpha_{l+1}|^2|P_l(\gamma_{l+1}z^2)|^2+2|\beta_{l+1}|^2|z^{-1}|^2|P_l(-\gamma_{l+1}z^2)|^2\\&=2|\alpha_{l+1}|^2|P_l(\gamma_{l+1}z^2)|^2+2|\beta_{l+1}|^2|P_l(-z^2)|^2,\ \forall z\in S^1. \qquad (58)\end{aligned}$$

for all $z \in S^1$. Since $|\alpha_{l+1}|=|\beta_{l+1}|$, the above equation becomes

$$2\left(|P_l(\gamma_{l+1}z^2)|^2+|P_l(-\gamma_{l+1}z^2)|^2\right)|\beta_{l+1}|^2\,. \qquad (59)$$

Noticing that $|\alpha_i|=|\beta_i|$ and $\gamma_i \in S^1$ ($i \in \{2\,,\,\dots\,,\,l\}$) and $\gamma_{l+1}z^2 \in S^1$ for any $z \in S^1$, we apply the induction assumption (57) of Step 2 to (59) and obtain

$$|P_l(\gamma_{l+1}z^2)|^2+|P_l(-\gamma_{l+1}z^2)|^2=2^l(|\alpha_1|^2+|\beta_1|^2)\prod_{i=2}^{l}|\beta_i|^2, \forall z \in S^1\,. \qquad (60)$$

Combining (60) and (59), we prove that

$$\begin{aligned}&|P_{l+1}(z\,;\,\alpha_{l+1},\beta_{l+1},\gamma_{l+1},...,\alpha_1,\beta_1)|^2\\&+|P_{l+1}(-z\,;\,\alpha_{l+1},\beta_{l+1},\gamma_{l+1},...,\alpha_1,\beta_1)|^2\\&=2^{l+1}(|\alpha_1|^2+|\beta_1|^2)\prod_{i=2}^{l}|\beta_i|^2|\beta_{l+1}|^2\\&=2^{l+1}(|\alpha_1|^2+|\beta_1|^2)\prod_{i=2}^{l+1}|\beta_i|^2 \qquad (61)\end{aligned}$$

which renders

$$\begin{aligned}&\max_{z\in S^1}|P_{l+1}(z\,;\,\alpha_{l+1}\,,\,\beta_{l+1}\,,\,\gamma_{l+1}\,,\,\alpha_1\,,\,\beta_1)|^2\\&\le \max_{z\in S^1}\big\{|P_{l+1}(z\,;\,\alpha_{l+1}\,,\,\beta_{l+1}\,,\,\gamma_{l+1}\,,\,\alpha_1\,,\,\beta_1)|^2\\&\qquad+|P_{l+1}(-z\,;\,\alpha_{l+1}\,,\,\beta_{l+1}\,,\,\gamma_{l+1}\,,\,\alpha_1\,,\,\beta_1)|^2\big\}\\&\le 2^{l+1}(|\alpha_1|^2+|\beta_1|^2)\prod_{i=2}^{l+1}|\beta_i|^2 \qquad (62)\end{aligned}$$

for all $z \in S^1$ and the parameters chosen from $(1)$ of (36).

## REFERENCES

[1] C. Rö$\beta$ing and V. Tarokh, "A construction of OFDM 16-QAM codewords having low peak powers", *IEEE Trans. Inform. Theory*, Vol. 47, No. 5, pp. 2091-2094, Nov. 2001.

[2] A.E. Jones, T.A. Wilkinson and S.K. Barton, "Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission schemes", *Electron. Lett.*, Vol. 30, No. 25, pp. 2098-2099, Dec. 1994.

[3] C.V. Chong, R. Venkataramani and V. Tarokh, "A new construction of 16-QAM Golay complementary sequences", *IEEE Trans. Inform. Theory*, Vol. 49, No. 11, pp. 2953-2959, Nov. 2003.

[4] S. Boyd, "Multitone signals with low crest factor", *IEEE Trans. Circuits Syst.*, Vol. CAS-33, No. 10, pp. 1018-1022, 1986.

[5] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences and Reed-Muller codes", *IEEE Trans. Inform. Theory*, Vol. 45, No. 7, pp. 2397-2417, Nov. 1997.

[6] J. A. C. Bingham, "Multicarrier modulation for data transmission: An idea whose time has come", *IEEE Commun. Mag.*, Vol. 28, No. 1, pp. 5-14, May 1990.

[7] X. Li and L. J. Cimini Jr., "Effects of clipping on the performance of OFDM with transmitter diversity", *Proc. IEEE VTC97*, pp. 1634-1638, May 1997.

[8] M. G. Parker and C. Tellambura, "Generalised Rudin-Shapiro constructions", *Electronic Notes in Discrete Mathematics, WCC2001 International Workshop on Coding and Cryptography*, Vol. 6, Paris, April 2001.

[9] M. An, J. Byrnes, W. Moran, B. Saffari, H. S. Shapiro and R. Tolimieri, "PONS, Reed-Muller codes, and group algebras", NATO Advanced Study Institute: *Computational Noncommutative Algebra and Applications*, Tuscany, Italy, July 2003.

[10] J. Zhao, "Efficient identification of the codewords with low peak-to-mean envelope power ratio of multicarrier transmission", *Proc. IEEE VTC04*, pp. 373-377, Sept. 2004.

[11] J. Zhao, "A peak-to-mean power control scheme–the extended Rudin-Shapiro construction", *Proc. IEEE VTC04*, pp. 621-625, Sept. 2004.

[12] D. Wulich, "Reduction of peak-to-mean ratio of multicarrier modulation using cyclic coding", *Electron. Lett.*, Vol. 32, No. 5, pp. 432-433, Feb. 1996.

[13] R. Bäuml, R. Fischer and J. Huber, "Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping", *Elect. Letts.*, Vol. 32, No. 22, pp. 2056-2057, Oct. 1996.